Network Analysis Tools

The Joint Advanced Distributed (JADS) Joint Test Force (JTF) uses several tools to assist in the setup and checkout of new networks, diagnose network problems, monitor the health and status of the network, and characterize network performance. This paper discusses these tools at a high level.

Silicon Graphics NetVisualyzer

SGI's NetVisualyzer is a suite of tools used for network analysis. The tools capture (snoop on) and examine network traffic. These tools are used during network setup to ensure that the network equipment are configured properly, the nodes are talking to each other as intended, and that extraneous network traffic is identified and minimized when possible.

NetVisualyzer uses centralized Display Stations and remote Data Stations. Data Stations are located on each wide area network segment to collect network data. The data from each Data Station is sent to a Display Station located in the Test Control and Analysis Center (TCAC) where the information can be processed and/or displayed. The Display Station software must be hosted on an SGI platform while the Data Station software can be hosted on SGI and Sun MicroSystems platforms.

The Display Station can collect data from the remote sites and a variety of tools can be used to display or analyze the data. The tools are Netlook; NetGraph; Netcollect, NetPack, and Net Account; NetSnoop; and Analyzer. Most of the tools allow for filtering of data by such criteria as protocol type, source, destination, or other user defined criteria.

Netlook presents an operator with a graphical display showing network traffic patterns across the entire JADS WAN. The traffic between specific hosts at each segment and between segments is shown. This tool is used during network setup and configuration to aid in the configuration of the network hardware and computer equipment on each segment. The tool helps determine if traffic is flowing through the network. Netlook is also used during a test to monitor the network and its component computers.

Using NetGraph, the data collected at each remote Data Station can be used to display characteristics for each local area networks (LAN). The tool can graphically depict traffic data such as percent of Ethernet bandwidth, packets per second, bytes per second, etc. The maximum and average statistics are given. This tool is used primarily to monitor the LANs during a test. The packets can be filtered in various ways to gain insights on network traffic of special interest.

NetCollect, NetPack, and NetAccount can be used to collect and process traffic to produce statistical reports on the network protocols. NetCollect will collect the local network traffic and store it locally. NetPack and NetAccount are used post-test to consolidate and process the data. The types of protocols and their relative size and quantity are a result of this process. This is used as a diagnostic tool.

NetSnoop is a tool that examines the protocol header information of each packet on the network. Information such as protocol type, source port and address, and destination port and address allow network engineers determine the flow of traffic on each LAN segment. This tool is available on the Data Stations. During the network setup, this tool is used to ensure that the computers are sending the data to the correct addresses and to verify that the routers are passing the data as intended. This is one of the most useful networking tools used at JADS.

Analyzer captures packets and provides the information available with NetSnoop. In addition, the actual packet header and data can be analyzed.

Cabletron Spectrum

Cabletron's Spectrum is a network management tool. Spectrum uses the Simple Network Management Protocol (SNMP) capabilities of the JADS network hardware to provide network performance data and to assist in finding and diagnosing network problems. Unlike NetVisualyzer, Spectrum accesses hardware, it does not examine or collect network traffic.

Spectrum has two components: SpectroServer and SpectroGraph. SpectroServer runs on a Sun SPARCStation 20. It polls the network for the desired data and stores the data in a database. SpectroGraph is the graphical user front end to Spectrum. Spectrograph is used when building the network model and database, specifying Spectrum data collection parameters, accessessing the database, preparing reports, and real-time monitoring of the network. Spectrograph is run on a Sun MicroSystems SPARCStation 5.

The basic Spectrum package supports only the standard SNMP capabilities. Most vendors have enhanced the capability of their systems to support SNMP. In order to adequately capture the required data, JADS purchased management modules for the equipment making up our network. For example, most of our routers use Cisco software, therefore, a Cisco management module was purchased. In addition, the WellFleet module was purchased because of routers in place at Pt. Mugu and China Lake.

The tool gives a graphical representation of the extended JADS network. Network or hardware problems can set off alarms that are displayed on the workstation screen. This allows the source of problems to be located quickly.

By using SNMP to query the hardware such as routers, network performance data such as bandwidth utilization on the WAN links or packets dropped by the routers can be collected. An operator can query the routers in real-time to monitor the status of the network during a test. Also, the data is stored in the Spectrum database and reports can be generated post-test.

Network General Sniffer

The Network General Sniffer is a portable protocol analyzer used to diagnosis network problems. The Sniffer can analyze traffic on a single Ethernet segment over an extended period of time. It provides a real-time statistical view of the protocols on the network. An operator can get a detailed picture of the protocols and network present on the segment. It is a diagnostic tool used to isolate network traffic problems and to ensure that undesirable traffic is not present. Additional hardware would allow the Sniffer to be used to analyze serial data lines.

IP Ping Utility

The ping utility that is part of most, if not all, TCP/IP stacks is a very simple but useful tool. The utility sends ICMP packets to a specified address and listens for the response. The round trip time is the output of this utility. The ping times provide a baseline of the latencies due to the network itself since the processing times associated with an ADS systems are not included. It is a quick and easy tool to determine if another system is up or to help isolate link losses. In general, the ping times are stable. If these times have large variances (determined by experience), a problem with the network usually exists.

Point of Contact:
Mr. Greg Grundhoffer, SAIC
JADS JTF
11104 Menaul Blvd, NE
Albuquerque, NM 87112-2454
grundhoffer@jads.kirtland.af.mil
(505) 846-0927
FAX: (505) 846-0603